# DOD Victim-Witness Assistance Program Training Conference

**MAJ Michelle E. Crawford**
**OTJAG, Criminal Law Division**
**Chief, Policy Branch**

# Outline of Instruction

- What is Identity Theft
- Minimizing your Risk
- What to do if You're a Victim
- Filing a Complaint
- Federal and State Laws
- Current Events
- Links and Publications

# What is Identity Theft?

- When someone co-opts (steals) your name, SSN, credit card number, or other personal information about you for their own use
- It occurs when someone appropriates your own information without your knowledge or consent to commit fraud or theft
- Identity theft is the top consumer fraud complaint in America
- Per our law enforcement personnel, 900,000 people will become victims this year

# How Do Identity Thieves Work?

- Going through your mail or trash to take pre-approved credit card offers, discarded credit card receipts or other personal information;
- Stealing your purse or wallet;
- Calling you on the phone to gain personal information including your name, date of birth, social security number;
- Looking over your shoulder at an ATM
- Family Member, Friends, & Friends of Friends

# What do they do with the Information?

- Open a new credit card account, using your name, date of birth, and Social Security number and when they don’t pay the bills, the delinquent account is reported on ***your*** credit report
- Call your credit card issuer, pretending to be you, and change the mailing address on your credit card account - because your bills are being sent to the new address, you may not immediately realize there's a problem
- Establish cellular phone service in your name
- Open a bank account in your name and write bad checks on that account
- **ETC, ETC, ETC**

# Minimizing Your Risk

- Do not carry your social security card, birth certificate or passport;
- Only keep a few credit cards in your purse or wallet when shopping;
- Keep a list of your credit card account numbers, with expiration dates and telephone numbers;
- Do the same for all your bank accounts;

# Minimizing Your Risk

## continued

- Always take credit card receipts for all purchases and store in a safe place, or dispose of by shredding/tearing;
- Use a mix of letters and numbers (not personal information such as your birth date, last four digits of your social security, or mother's maiden name) when creating passwords and PIN's for important accounts;
- Do not store passwords in your purse or wallet!

# What to do if You're a Victim?

- How do you know if you're a Victim?
  - ✓ Your credit card statements show unauthorized charges and/or purchases that you know you did not make;
  - ✓ You fail to receive bills or credit card statements for charges you have made, when in the past you received them at the same time each month;
  - ✓ You are receiving phone calls from creditors trying to collect debts that are not yours

# What to do if you're a Victim? - continued

1. Contact the fraud departments of each of the three major credit bureaus and report that your identity has been stolen. Ask that a "fraud alert" be placed on your file and that no new credit be granted without your approval.

2. For any accounts that have been fraudulently accessed or opened, contact the security departments of the appropriate creditors or financial institutions. Close these accounts. Put passwords (***not*** your mother's maiden name) on any new accounts you open.

3. File a report with your local police or the police where the identity theft took place. Get a copy of the report in case the bank, credit card company, or others need proof of the crime later on.

# Filing a Complaint

- Local Law Enforcement/MPs (SPs, etc)
- The FTC serves as the federal clearinghouse for complaints by victims of identity theft **(complaint form)**
- FTC does not resolve individual consumer problems, but complaint helps investigate fraud, and can lead to law enforcement action
- The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies worldwide

# Federal Laws

- **Identity Theft and Assumption Deterrence Act**
  - ✓ In October 1998, Congress passed the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act) to address the problem of identity theft. Specifically, the Act amended 18 U.S.C. § 1028 to make it a federal crime when anyone:
  - ✓ knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.
- Violations investigated by federal investigative agencies such as the U.S. Secret Service, the FBI, and the U.S. Postal Inspection Service
- Violations prosecuted by the Department of Justice

# Federal Laws
## continued

- Fair Credit Reporting Act
- Fair Credit Billing Act
- Fair Debt Collection Practices Act
- Electronic Funds Transfers Act

# State Laws

- 48 out of 50 states, plus Guam have statutes RE: ID Theft
- Many have civil and criminal liability
- CO, VT, DC and USVI do not have specific ID Theft law

# Current Events

- December 2002: 500,000 military and family members had personal information (including SSNs, home addresses, etc) stolen from the TRICARE servicing center for the central region (TriWest Healthcare Alliance)
- Victims:
  - Likely a victim if received civilian healthcare through TRICARE between Dec 99-Dec 02 in 16 states
  - Should have gotten 2 letters from TriWest Healthcare Alliance if DEERS info is up to date (early Jan 03 and mid-Feb 03)…can also check http://triwest.com/, select **ALERT** box, then select **Personal Information Verification Form**
  - Central point to request Fraud Alert or initial Credit Reports = https://triwest2.triwest.com/announcement/search/

# Current Events - continued

- Per the TriWest POC, as of 18 March 2003, apparently no ID theft cases have currently been tracked back to this incident
- If you think you're affected, but didn't get either letter:
  - Go to secure website to check; also one stop way to have all 3 Credit Bureaus place Fraud Alert and send current credit report
  - Must submit name exactly as it appeared on the TRICARE card
  - Must enter family member's last four (NOT sponsor's)
  - FTC recommends people at risk should request copies of credit reports every 3 months for the first year after being placed at risk (creditors not bound by Fraud Alerts placed by Credit Bureaus)

# Links and Publications

- Federal Trade Commission

  **www.consumer.gov/idtheft/victim**

with useful ID Theft Affidavit

- U.S. Treasury

  **www.ustreas.gov/tigta**

- U.S. Postal Service

**www.usps.com/postalinspectors/fraud/identitytheft**

# ??
# Questions ??